以下は ZDNet ニュースで紹介された ReadNotify に関連する記事の和訳と原文です。
（源データ；http://news.zdnet.com/2100-1009_22-6121048.html）

# HP 社、情報漏洩対策に ReadNotoify 社のサービスを利用

By Joris Evers, CNET News.com

Published on ZDNet News: September 28, 2006, 6:18 PM PT

**ヒューレット･パッカード社は商用のメール追跡サービスを使って CNET News.com レポーターに追跡指定したファイルを送信した、と HP 調査員は木曜日に公聴会で証言**

米国ヒューレット･パッカード社（HP）の調査員 Fred Adler 氏は、ReadNotify.com サービスを使って CNETの Dawn Kawamoto レポーターにメールを送り、彼女の情報源を明らかにしようとしたと連邦下院議会分科会で証言。

Adler 氏の証言は、同社がどの様に追跡指定したメールを Kawamoto 氏に送信したかについて HP 役員会議でのドラマ発生以来初めて説明したもの。Adler 氏は、会社は継続して何らかの問題に対して追跡メールを使っているとも述べた。

「これは以前からやっていましたし、依然として会社の方針です。私の上司も調査ツールとして認めています。私達は盗まれた製品の場所を特定する為にこれを使って来ました。この方法で法の執行もサポートして来ました。」と Adler 氏。

調査員は ReadNotify 社が提供する追跡メカニズムを使って、メールに添付した文書を誰が開いたかを知ることができる。今回の使用目的は、Kawamoto 氏が受信したメールを彼女の情報源に転送するに違いないという見込みの上で追跡情報を彼女に送り、HP の機密情報の漏洩源を突き止めることだった。

「ReadNotify を使えばメールの添付文書を誰がいつ開いたか、使用したインターネットプロトコル、その IP アドレスを知ることができます。IPアドレスが分かればユーザの地理的位置やインターネット接続に使ったインターネットサービスプロバイダーも分かります。」と Adler 氏。

「私達は Keyworth 氏が追跡指定した情報の受け手だろうと疑っていました。」と Adler 氏。Keyworth 氏はHPの取締役で、メディアに情報を漏洩していたことを認めている。

先週の HP 本社での記者会見で、Michael J. Holston 氏(HP が雇った弁護士)は、このメール操作によって今回の訴訟に至った訳ではないと言った。


ReadNotify はオンラインサービスであり、そのサービスサイトによると、誰でも無料で試用の追跡メールを25メール送れる。利用料金は年間 24 ドル。そのプレミアムサービスの利用料は年間 36 ドルで、MSオフィス文書や PDF ファイルを追跡できる。 類似サービスとして MailTracking.com がある。

ReadNotify では、単にマウスをポイントしクリックするだけでメールを追跡できる。 ReadNotify のサービスサイトではイメージが入った追跡因子も作成できる。この追跡因子のイメージ、緑色のチェックマークは、追跡する文書中にドラッグ＆ドロップでき、文書上にドロップした後見えなくなる。

ユーザは ReadNotify に自分のメールアドレスを登録し、追跡したいメールの送信アドレスの後に、「.readnotify.com」を付加する。このメールの受信者にはこの付加情報は見えないが、メールヘッダを見ればそのメールが ReadNotify を中継していることが分かる。

ReadNotify のサービスサイトによれば、既定値の設定では受信確認のメッセージがポップアップするかも知れないので、受信者は何かあるなと気が付くかも知れないが、気付かない様にする「見えない追跡」設定もあるとのこと。

ReadNotify には複数の追跡オプションがある。利用者は追跡指定したメールや文書を開いた人のIPアドレス、何時それを開いたか、その詳細を見ることができる。このサービスは PC とメールプログラムに関するデータも示す。メールやファイルを転送したなら、転送先に関する同様のデータも表示する。

ReadNotify は Web バグとして知られている技術を使っている様だ。この技術は複数のメールマーケッターが既に使っている。ReadNotify を使って送ったメールや文書はサービスがホストするサーバへの隠れたリンクを含んでおり、このメールや文書を開くと追跡因子が ReadNotify サーバに開いた事を教える。

普通のユーザはこれに気づかない様だ。メールは HTML 言語で精密につくられ、追跡因子は見えない。Notepad のようなプログラムを使えば追跡因子のサーバへのリンクは見えるだろう。ファイアウォールはこれに対する警報を Web ユーザに出すことができるかも知れない。

豪州、シドニーにある ReadNotify 社のＣＴＯである Chris Drake 氏はメールインタビューで「ReadNotify は最大 36 の異なった追跡技術の組合せを使います。これらが種々のメールクライアントやオペレーティングシステムに対応して機能し、その結果弊社のサービスはインターネット上で最も強力で、信頼性の高い追跡サービスになっています。ReadNotify は単純な Web バグ以上の技術を使っています。今では優秀なメールプログラムは全てこの様なバグをブロックし、ほとんどのアンチスパムソフトはバグを拒絶しているので、弊社はこの様な非常に単純な追跡技術はもう使っていません。」と言っている。

木曜日の連邦議会の証言では、追跡因子をメールに含めることが正当かどうかについて質問があった。

HP の社外弁護士 Larry Sonsini 氏はワシントン州民主党 Jay Inslee 議員の質問に対して「本件に関する明確な法律の規定は無いと思います。これは、どう使うかによって連邦や州の法律に関ってくると思います。」と答えた。

ReadNotify 社はそのサービスサイト上で、使用条件としてサービスを「合法な目的」だけのために使うように規定している。同社は更に、その製品を「詐欺を意図したメール」には使わない様に利用者に要求している。

Drake 氏は「弊社はプライバシと法的問題との関係について質問を受けることがあります。ReadNotify 社は、メールの作成者は自分が作ったメールについて、そのメールの追跡を含めて主体的に何でもできると信じています。最も大事なのは、メールの受信者は自分のインボックスに入ったメールが自分のものではないのだと認識することです。メールを書いた人は自分の労力を使って自分が

**考えたことを纏め、それをメールの中に込めていますから、メールはそれを作った人のものです。文書についても同様です。」と言った。**

ReadNotify **社はサービスを通して自社の顧客の動きを監視している訳ではない。**Drake **氏はサービスに関する質問に対して「弊社は法の執行機関が、オンライン犯罪とオンラインに関連する現実世界の犯罪行為両方に対処する為に弊社のサービスを広く使っていることを知っています。2 年前に非常に興味深い事件がありました。子供が誘拐され、弊社のサービスを使ってメールを追跡し、世界の何処でそのメールを開いたかを知ることができ、子供を無事保護することができました。ReadNotifyサービスが子供の誘拐事件の解決に貢献したのです。」と自信を持って答えた。**

**ＨＰ社が役員会議の情報漏洩に関する調査で追跡サービスを使ったことは、同社の違法な可能性がある複数の手段の１つだ。このカルフォルニア州パロアルトの企業は"pretexting"(個人の記録を得る為に不正な手段を取ること)な手法を取ったことに対しても批判を受けている。**

**木曜日の証言では、CEO Mark Hurd 氏は、消費者のプライバシ保護に対する動きに対して、追随するのではなくリードすることが会社にとって重要だと述べ、メール追跡機能の使用に関して「私はこの技術を検討し、この技術を使ったメールの送受信について個別に調べ、全く問題が無いことを明確にしたいと思います。」と言った。**

Adler **氏の証言は、一日中続いた下院の** Energy and Commerce Committee **の調査分科会によるＨＰ社のスパイスキャンダルに関する公聴会の一部。**Hurd **氏と元会長** Patricia Dunn **氏は証言したが、他の何人かの** HP **従業員と外部契約者は自己負罪に対して憲法修正第** 5 **条の適用を要求した。**

……

**以下、ニュースの原文**（参考；http://news.zdnet.com/2100-1009_22-6121048.html）

# How HP bugged e-mail

By Joris Evers, CNET News.com

Published on ZDNet News: September 28, 2006, 6:18 PM PT

**Hewlett-Packard employed a commercial service that tracks e-mail paths to bug a file sent to a CNET News.com reporter, an HP investigator said Thursday.**

HP investigators used the services of ReadNotify.com to trace an e-mail sent to reporter Dawn Kawamoto in an attempt to uncover her source in a media link, Fred Adler, an HP security employee, said during testimony before a U.S. House of Representatives subcommittee.

Adler's testimony, for the first time since the HP boardroom drama erupted, specified how the company bugged the e-mail it sent to Kawamoto. Moreover, Adler said that it's still company practice to use e-mail bugs in certain cases.

**"That was and still is current policy," he said. "It still is sanctioned by my management as an investigative tool, we have used it in the past for investigations, for determining the locations of stolen product and what-not, and we have also assisted law enforcement."**

The tracking mechanism provided by ReadNotify would allow investigators to see who opened the file attached to the e-mail, Adler said. The objective was to determine whether the journalist would forward the e-mail to her source, and to then determine the source of the leaks of HP confidential information.

Through ReadNotify, investigators would see when the e-mail attachment was opened and the Internet Protocol, or IP, address of the computer it was opened on, Adler said. An IP address can disclose the geographic location of a user, as well as the Internet service provider used to connect to the Internet.

"We suspected it would be Mr. Keyworth that would be the recipient," Adler said, referring to George Keyworth, the HP board member who has admitted he leaked information to the media.

During a press conference at HP headquarters last week, Michael J. Holston, a lawyer hired by HP, said that bugging e-mail did not yield results in this case.

ReadNotify, which operates as an online service, provides a free trial that lets anyone send 25 bugged e-mails, according to its Web site. Subscriptions are offered starting at $24 per year. A premium $36-a-year subscription is required to bug files such as Office and PDF documents. A similar service operates as MailTracking.com.

ReadNotify's service makes bugging e-mail a matter of pointing and clicking. The ReadNotify Web page will generate a document with an image. This image, a green check mark, can simply be dragged and dropped into the document that needs to be traced. The check mark becomes transparent after being dropped.

Users of the service register their e-mail addresses with ReadNotify, then simply append ".readnotify.com" to any e-mail address they send mail to if they want the message to be tracked. Recipients won't see this suffix, but could tell from the e-mail headers that the message was relayed.

In the default ReadNotify setting, an e-mail recipient could discover something is awry because a return receipt message may pop up, but the service also has an "invisible tracking" setting, according to the Web site.

ReadNotify offers a range of tracking options. Users can see the IP addresses of those who opened bugged e-mails or documents, including details on when the mail or file was opened.

The service also shows some data on the PC and e-mail program. If the mail or file was forwarded, it shows the same data on that person.

The ReadNotify service appears to use what's known as a Web bug, a technique also employed by some e-mail marketers. An e-mail or a document sent through ReadNotify includes hidden links to one or more files hosted by the service. When the message or the file is opened, the program retrieves the files and by doing so checks in with ReadNotify.

A typical recipient will not notice this. The e-mail is crafted in HTML, or Hypertext Markup Language, and the tracer files are not visible. The actual links that retrieve the files will only show when viewing the source of the e-mail, for example through a program like Notepad. A firewall could alert the user of the Web traffic, however.

"ReadNotify uses a combination of up to 36 different simultaneous tracking techniques," Chris Drake, the company's Sydney, Australia-based chief technology officer said in an e-mail interview. "One or more of these usually works in all different e-mail clients and operating systems, making us the most powerful and reliable tracking service on the Internet."

In short, ReadNotify uses more technologies than simple Web bugs, Drake said. "All good e-mail programs have blocked these now and most anti-spam programs reject them too, so we no longer rely on this simplistic tracking idea."

During testimony before Congress on Thursday, the legality of including a bug in e-mail messages was questioned.

**"I think the law regarding that is not as clear as it should be," Larry Sonsini, HP's outside lawyer, said in response to questions from Rep. Jay Inslee, a Washington state Democrat. "Depending on how it is used and the methodologies, it could very well implicate federal or state statutes," Sonsini said.**

**In the terms of use posted on its Web site, ReadNotify stipulates that its services should be used for "lawful purposes only." The company goes on to say that its product should not be used to transmit "intentionally deceptive e-mail messages."**
**"Occasionally, we're asked about privacy and legal issues," Drake said. Essentially, ReadNotify believes an e-mail author can do whatever he pleases with the message, including tracking it. "It is important to understand firstly that just because an e-mail comes into your inbox, it does not make it yours. When a person puts the effort into thinking up an e-mail and composing it: that e-mail is theirs."**

ReadNotify doesn't monitor its clients, but Drake has had praise and questions about the service, he said. "We do know that we are heavily used by law enforcement in combating both online

crime, and real-world crime that has online aspects," Drake said. **"The most interesting event was about two years ago, when our service helped recover a kidnapped child when a tracked e-mail provided an international location that led to a safe recovery."**

Use of the e-mail bug is one of the possibly illegal methods used in HP's investigation into boardroom leaks. The Palo Alto, Calif., company is also facing heat over the use of "pretexting," which refers to the use of fraudulent means to obtain someone else's personal records.

**In testimony Thursday, CEO Mark Hurd said it is important for the company to lead, not follow when it comes to consumer privacy. "I am going to go back to that technology and look specifically at every use of that kind of send-receive technology and make sure there is absolute clarity," he said of the use of e-mail tracing.**

Adler's testimony was part of a full day of hearings into the HP spying scandal by an oversight and investigations subcommittee of the House of Representatives' Energy and Commerce Committee. Hurd and former Chairman Patricia Dunn also testified, but several other HP employees and contractors invoked their Fifth Amendment rights against self-incrimination.